

安全防火墙FTD — 缩放电话音频阻止列表 ；由于旧的VDB

目录

问题

用户遇到呼叫连接但音频丢失的Zoom Phone呼叫音频问题。FTD正在丢弃来自Zoom IP范围的UDP媒体数据包，在数据包捕获和ASP丢弃计数器中显示这些数据包是由Snort列出的块。

具体症状包括：

- 防火墙运行思科漏洞数据库(VDB)427版或更低版本。
- 防火墙包含一个访问规则，该规则必须根据Firepower数据库提供的默认Zoom/RTP应用ID允许缩放流量。根据appid.cisco.com，规则必须允许所有这些端口通过Zoom AppID:
 - UserZoom(6243):80,443/tcp
 - Zoom Download(4628):80,443/tcp
 - 缩放上传(4627):80,443/tcp
 - 缩放会议(4629):80/tcp
 - RTP音频(2475):5004/udp
 - SIP(426):5060/udp
- 但是，Packet Tracer输出显示流量因阻止列表原因“被防火墙预处理器阻止或列入黑名单”而被丢弃。

```
<#root>
```

```
Phase: 17  
Type: SNORT  
Subtype: firewall
```

```
Result: DROP
```

```
Elapsed time: 345716 ns  
Config:
```

Network 0, Inspection 0, Detection 4, Rule ID 268434438

Additional Information:

Starting rule matching, zone 3 -> 3, geo 840 -> 840, vlan 0, src sgt: 0, src sgt type: unknown, ds

Matched rule ids 268434438 - Block

Result:

input-interface: Outside(vrfid:0)

input-status: up

input-line-status: up

output-interface: Outside(vrfid:0)

output-status: up

output-line-status: up

Action: drop

Time Taken: 640578 ns

Drop-reason: (firewall) Blocked or blacklisted by the firewall preprocessor, Drop-location: frame

- 数据包捕获显示丢弃原因：“snort-blacklist”。

<#root>

40: 22:52:36.383692 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

141: 22:52:36.383723 206.247.118.57.60030 > 10.X.X.1.9178: udp 103

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

142: 22:52:36.385188 206.247.118.57.60030 > 10.X.X.1.9178: udp 44

Drop-reason: (snort-blacklist) Packet is blacklisted by snort

, Drop-location: frame inspect_dp_snort_snp_drop_frame_wcaller:61 flow (NA)/NA

- 在system support trace输出中，由于应用标识处于挂起状态，流量在规则匹配期间被延迟。但是，流量被错误识别并被阻止。IP地址是根据Zoom文章[Zoom network firewall or proxy server settings](#)要求访问的Zoom公共IP。

<#root>

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

pending rule order 12, 'allow-outbound', AppID

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

Deferring trust until a rule is matched

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

match rule order 28, 'Default Block', action Block

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 MidRecovery data sent for rule id: 26843

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Matched a rule, stop deferring trust

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Generating an SOF event with rule_id = 2

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1

deny action

10.X.X.1 9476 -> 206.247.118.12 24794 17 AS=0 ID=1 GR=1-1 Deleting Firewall session flags=0x20, 1c

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Packet 17168248: UDP, 04/14-14:44:53.110

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Firewall: starting rule matching, zone 1

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Firewall: block rule, 'Default Block', force_block

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

AppID: service: (-1), client: (0), payload: (0), misc: (0)

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Stream: pending block, drop

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1 Policies: Network 0, Inspection 0, Detect

206.247.118.12 24794 -> 10.X.X.1 9476 17 AS=0 ID=1 GR=1-1

Verdict: blacklist

- 当缩放IP尝试响应时，系统支持跟踪指示“RTP客户端候选返回错误 — 无效(-11)”和“第三方返回未知(0)”消息。

<#root>

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1 New AppId session

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

3rd party returned unknown (0)

206.247.118.55 54808 -> 10.X.X.1 9824 17 AS=0 ID=2 GR=1-1

RTP client candidate returned error-invalid (-11)

10.X.X.1 9824 -> 206.247.118.55 54808 17 AS=0 ID=2 GR=1-1 app event changes: created

- FTD show asp drop命令显示阻止列表丢弃的快速增量。

<#root>

Frame drop:

-----ABBREVIATED-----

Blocked or blacklisted by the firewall preprocessor (firewall)	11224
Blocked or blacklisted by the stream preprocessor (stream)	2354
Fragment reassembly failed (fragment-reassembly-failed)	3
Packet is blacklisted by snort (snort-blacklist)	27173
Packet is blocked as requested by snort (snort-block)	42

环境

- 由FMC管理的思科Firepower FTD版本7.7.11
- 漏洞数据库(VDB)版本427或更低版本
- Snort版本3.3.5.1100-66
- 主要影响缩放IP子网170.114.0.0/16和206.247.0.0/16的流量，但可以包括其他缩放IP

分辨率

Cisco Bug ID CSCwu22106解决方法 — 预过滤器规则实施

1:为缩放流量创建预过滤器规则。

导航到Policies > Access Control > Prefilter并使用此配置创建新规则：

- 规则名称:缩放预滤器
- 操作：快速路径
- 源区域:输入界面

- 目标区域:输出接口
- 源地址：any
- 源端口：any
- 目的地址：缩放IP范围(170.114.0.0/16、206.247.0.0/16)和缩放网络防火墙或代理服务器设置中所述的任[何其他范围](#)。
- 目的端口：UDP 10000-64000

2:备用访问控制规则配置

如果不首选预过滤，请通过删除Zoom应用标识符并使用显式IP和端口匹配来修改现有的访问控制策略规则：

- 规则名称:Zoom-Allow
- 操作：允许
- 源区域:输入界面
- 目标区域:输出接口
- 源地址：any
- 源端口：any
- 目的地址：缩放IP范围(170.114.0.0/16、206.247.0.0/16)和缩放网络防火墙或代理服务器设置中所述的任[何其他范围](#)。
- 目的端口：UDP / “Zoom-Phone-Ports” (范围10000 64000)
- 日志记录: (可选，用于监控允许的流量)

3:将配置更改部署到FTD设备，并验证双向音频功能是否已恢复。

- 监控ASP丢弃计数器以确认阻止列表已停止：

```
device# show asp drop
```

- 检查数据包捕获，确保双向流量成功：

```
device# show capture
```

4:缺陷Cisco Bug ID CSCwu22106已在思科漏洞数据库(VDB)版本428中解决。Firepower设备必须运行最新的VDB版本以避免此缺陷的影响。同样，相关的缺陷Cisco Bug ID CSCwn80786在VDB版本395中已解决。

原因

漏洞数据库(VDB)版本427中的Cisco安全防火墙应用识别签名存在缺陷，导致Zoom Phone媒体流量被错误分类，随后被Snort检测引擎阻止。此行为在Cisco Bug ID CSCwu22106和相关缺陷Cisco Bug ID CSCwn80786下跟踪，该缺陷记录了使用应用ID时Zoom IP地址和媒体流的不正确处理。

相关内容

- [缩放网络防火墙或代理服务器设置](#)
- [快速路径预过滤的最佳实践](#)
- [Cisco Bug ID CSCwu22106 — 在VDB 427中错误处理Zoom IP地址](#)
- [Cisco bug ID CSCwn80786 — 缩放应用检测器无法检测到用于缩放电话的网络](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。